

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOSHUA LEVIN
705 Spruce Street
Philadelphia, PA 19106
Plaintiff

v.

LOWER MERION SCHOOL DISTRICT
301 East Montgomery Avenue
Ardmore, PA 19003

and

THE BOARD OF DIRECTORS OF THE
LOWER MERION SCHOOL DISTRICT
301 East Montgomery Avenue
Ardmore, PA 19003

and

CHRISTOPHER W. MCGINLEY
Superintendent of Lower Merion School District
301 East Montgomery Avenue
Ardmore, PA 19003
Defendants

NO.

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff, Joshua Levin, by way of Complaint against the Lower Merion School District, the Board of Directors of the Lower Merion School District, and Christopher W. McGinley, Superintendant of the Lower Merion School District, upon information and belief, allege as follows:

JURISDICTION AND VENUE

1. Plaintiff brings this action pursuant to §§ 2511 and 2520 of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2511 and 2520, § 1030 of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, § 2701 of the Stored Communication Act (“SCA”), 18 U.S.C. § 2701, § 1983 of the Civil Rights Act, 42 U.S.C. § 1983, The Fourth Amendment of the United States Constitution, U.S. CONST. amend. IV, the Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. C.S.A. § 5701 e seq. (“PWESA”), and Pennsylvania common law.

2. This Court has original jurisdiction over Plaintiff’s federal law claims pursuant to 28 U.S.C. §§ 1331 and 1337, and supplemental jurisdiction over Plaintiff’s state law claims pursuant to 28 U.S.C. § 1367.

3. Venue is proper in this district pursuant to 28 U.S.C. §1391(b) and (c) as each Defendant is a resident of and/or maintains a permanent business office in this district.

THE PARTIES

4. Plaintiff, JOSHUA LEVIN, is a citizen of the Commonwealth of Pennsylvania, residing at 705 Spruce Street, Philadelphia, PA 19106.

5. At the time of the operative facts, Plaintiff, Joshua Levin was a minor and a high school student attending Harriton High School at 600 North Ithan Avenue, Rosemont, Pennsylvania, 19010. Harriton High School is part of the Lower Merion School District.

6. Defendant, Lower Merion School District (“School District”), is a municipal corporation body politic within the Commonwealth of Pennsylvania with a principal place of business at 301 East Montgomery Avenue, Ardmore, Pennsylvania, 19003.

7. Defendant, Board of Directors of the Lower Merion School District (“Board”), is comprised of a nine (9) member board elected locally to act as a corporate body in fulfilling the School District’s and the Commonwealth of Pennsylvania’s obligation to provide public education. The Board can be contacted through its secretary, Fran Keaveney, with an address of 301 East Montgomery Avenue, Ardmore, Pennsylvania, 19003.

8. Defendant, Superintendent of Schools Christopher W. McGinley (“McGinley”), is a School District Administrator appointed by the Board to supervise the day-to-day operation of the School District. As such he is responsible for the implementation of policies, procedures and practices instituted by the Board. The School District, the Board and McGinley are hereinafter collectively referred to as “Defendants.”

NATURE OF THE ACTION

9. While a student, Plaintiff, Joshua Levin, was issued a personal laptop computer equipped with a web camera (“webcam”) by the Lower Merion School District. Plaintiff seeks to recover damages caused to the Plaintiff for invasion of Plaintiff’s privacy, theft of Plaintiff’s private information and unlawful interception and access to acquired and exported data and other stored electronic communications in violation of the Electronic Communications Privacy Act, The Computer Fraud Abuse Act, The Stored Communications Act, § 1983 of the Civil Rights Act, The Fourth Amendment of the United States Constitution, the Pennsylvania Wiretapping and Electronic Surveillance Act and Pennsylvania common law.

10. Unbeknownst to Plaintiff, and without his authorization, Defendants had been spying on the activities of Plaintiff by Defendants’ indiscriminant use of and ability to remotely activate the webcams incorporated into each laptop issued to students by the School District.

This continuing surveillance of Plaintiff's home use of the laptop issued by the School District, including the indiscriminant remote activation of the webcams incorporated into each laptop, was accomplished without the knowledge or consent of the Plaintiff.

11. In connection with the acts and conduct complained of, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet.

OPERATIVE FACTS

12. In the Superintendent of School's welcome address appearing on the Lower Merion School District website as of the date hereof the Superintendent states as follows:

The District is also in the final stages of implementing a one to one laptop computer initiative at the High Schools. Thanks in part to State and Federal grants secured by our technology staff during the past few years, every high school student will have their own personal laptop-enabling an authentic mobile 21st Century learning environment. The initiative, which was launched with great success at Harrington last year, enhances opportunities for ongoing collaboration, and ensures that all students have 24/7 access to school based resources and the ability to seamlessly work on projects and research at school and at home. The result: more engaged, active learning and enhanced student achievement. While other districts are exploring ways to make these kinds of incentives possible, our programs are already in place, it is no accident that we arrived ahead of the curve; in Lower Merion, our responsibility is to lead.

13. As part of this initiative as indicated by the Superintendent, laptop computers equipped with webcams were issued on a one-to-one basis to all high school students in the School District. Plaintiff was one of these students and received a laptop for school purposes in September 2008.

14. An examination of all of the written documentation accompanying the laptop, as well as any documentation appearing on any website or handed out to students or parents concerning the use of the laptop, reveals that no reference is made to the fact that the school

district had the ability or intention of remotely activating the embedded webcam at any time in order to intercept images from the webcam of anyone or anything appearing in front of the camera at the time of the activation.

15. Unbeknownst to Plaintiff, the School District not only had the ability to remotely activate the webcam contained in a student's personal laptop computer issued by the School District at any time it chose and to view and capture whatever images were in front of the webcam, all without the knowledge, permission or authorization of any persons then and there using the laptop computer, but the School District utilized those capabilities and did exactly that.

16. Additionally by virtue of the fact that the webcam could be remotely activated at any time by the School District, the webcam would capture anything happening in the room in which the laptop computer was located, regardless of whether Plaintiff was even sitting at the computer and using it.

17. Plaintiff kept the laptop in his bedroom, as well as throughout his mother's household and his father's household. Plaintiff's younger brother noticed that the light in the camera would go off and on at odd times, wondering if the family was being "spied on". Plaintiff's mother dismissed this idea as absurd, as the notion that the school district was secretly monitoring and taking pictures of students was simply incomprehensible and beyond all rational belief. Plaintiff's father was told and believed that the light meant the laptop was "charging".

18. Unfortunately, this suspicion on the part of Plaintiff's younger brother was not a "fantasy", but was shockingly correct. Plaintiff's parents (and Plaintiff by separate correspondence) were for the first time informed of the above-mentioned capability and practice by the School District when they received a letter from Henry E. Hockeimer, Esquire, counsel for the School District, dated June 8, 2010, that stated, in part, as follows:

This letter is being sent to notify you that a recently completed investigation into the remote monitoring of laptop computers by the Lower Merion School District has revealed that the School district has captured webcam photographs and screenshots from a laptop that the District issued to your child, Joshua Levin. Specifically, **4,404 webcam photographs and 3,978 screenshots** that were recovered in the investigation were taken from your child's laptop from September 22, 2008 to March 12, 2009. Your child and you may view the recovered webcam photographs and screenshots, if you so desire. (emphasis added)

19. Furthermore, the aforesaid letter stated that if he so chose, Plaintiff had to view the recovered images at the United States Courthouse, on June 17, 2010 from 3:20 p.m. to 4:20 p.m.

20. Plaintiff opted to view the recovered images, and was shocked, humiliated and severely emotionally distressed at what he saw.

**COUNT I - INTERCEPTION OF
ELECTRONIC COMMUNICATIONS UNDER THE ECPA**

21. Plaintiff repeats and re-alleges each and every allegation above as if fully set forth herein.

22. Plaintiff asserts this Count against all Defendants, jointly and severally, pursuant to §§ 2511 and 2520 of the ECPA, 18 U.S.C. §~ 2511 and 2520.

23. Section 2511 of the ECPA provides in part;

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept, or endeavor to intercept, any... electronic communications;

(d) intentionally uses, or endeavors to use, the contents of any. . . electronic communication knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection; . . . shall be punished as provided in subsection (4) or shall be subject

to suit as provided in subsection (5).

24. Section 2520 of the ECPA provides in part;

(a) In general. —Except as provided in section 2511 (2)(a)(ii), any person whose... electronic communication is intercepted or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate

(b) Relief.—in the action under this section, appropriate relief includes —

(1) such preliminary and other equitable or declaratory relief as may be appropriate

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably' incurred.

25. Section 2510 of the ECPA, setting forth the definitions of the terms in § 2511, defines "person" to include "any employee, or agent of the United States or any State or political subdivision thereof. ... " 18 U.S.C. § 2510(6). Accordingly, each Defendant is a "person" within the meaning of § 2511.

26. Section 2510 defines "electronic communication" to include "any transfer of signs, signals, writing, imaging, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo electronic, or photo optical system that affects interstate or foreign commerce" is U.S.C. § 2510(12). Accordingly, the webcam images complained of constitute an "electronic communication" within the meaning of § 2511.

27. Section 2510 defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Section 2510 defines "electronic, mechanical,

or other device” to mean “any device or apparatus which can be used to intercept a wire, oral, or electronic communication” subject to exclusions not relevant to this action. 18 U.S.C. § 2510(5).

28. The software/hardware used by the School District to remotely activate the webcam complained of constitute an “electronic ... device” within the meaning of 18 U.S.C. § 2510(5). By using said software/hardware to secretly obtain webcam images, each Defendant “intercepts” that communication within the meaning of § 2511.

29. By virtue of the foregoing, Plaintiff is a “person whose ... electronic communication is intercepted..., or intentionally used in violation of this chapter” within the meaning of § 2520.

30. By virtue of the foregoing, Defendants are liable to Plaintiff for their violations of §§ 2511 and 2520 of the ECPA,

31. Since Plaintiff first learned of Defendants’ unlawful remote activation of the webcams complained of on June 8, 2010, this action is timely and not beyond ECPA’s applicable statute of limitations

32. Defendants’ actions complained of herein were conscious, intentional, wanton and malicious, entitling Plaintiff to an award of punitive damages.

**COUNT II- THEFT OF
INTELLECTUAL PROPERTY UNDER THE CFAA**

33. Plaintiff repeats and re-alleges each and every preceding allegation as if fully set forth herein.

34. Plaintiff asserts this Count against Defendants, jointly and severally, pursuant to § 1030 of the CFAA, 18 U.S.C. § 1030.

35. Section 1030 provides in part:

(a) Whoever -

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief . . . - No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

36. Section 1030 of the CFAA defines the term “protected computer” to include “a computer. . . which is used in interstate or foreign commerce or communication” 18 U.S.C. ~ 1030(e)(2)(B). Each laptop issued by the School District and equipped with a webcam is used in interstate communications and is therefore a “protected computer” within the meaning of § 1030.

37. Section 1030 of the CFAA defines the term “exceeds authorized access” to mean] “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). By using software/hardware to remotely activate the webcams complained of and intercept their images, each Defendant has gained “access a computer without authorization or exceeds

authorized access” within the meaning of § 1030.

38. By virtue of the foregoing, Defendants are liable to for their violations of § 1030 of the CFAA.

39. Since Plaintiff first learned of Defendants’ remote activation of the webcams complained of on June 8, 2010, this action is timely as to Plaintiff.

40. Defendants’ actions complained of herein were conscious, intentional, wanton and malicious entitling Plaintiff to an award of punitive damages.

**COUNT III - STORED
COMMUNICATIONS ACT (18 U.S.C. § 2701)**

41. Plaintiff repeats and re-alleges each and every preceding allegation as if fully set forth herein.

42. Section 2701 of the SCA provides, in pertinent part:

Except as provided in subsection (c) of this section, whoever --

1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

43. Section 2711 of the SCA defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo electronic or photo optical system that affects interstate or foreign commerce. . .” 18 U.S.C. §§ 2711, 2510(12). Accordingly, the webcam images complained of are “electronic communications” within the meaning of the SCA.

44. Section 2711 of the SCA defines “person” to include “any employee, or agent of the United States or of a State or political subdivision thereof, and any individual, partnership association. . . .” 18 U.S.C. § 2711, 2510(6). Accordingly, all Defendants are “persons” within the meaning of the SCA.

45. Section 2711 of the SCA defines “electronic storage” to include “any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof . . . 18 U.S.C. §§ 2711, 2510(17)(A)

46. Defendants’ use of the software/hardware to remotely activate the webcams complained of and to obtain their images constitutes an unauthorized acquisition of stored electronic communications in violation of the SCA.

47. Section 2701(b) of the SCA provides punishment in those instances where the unauthorized acquisition of stored electronic communications was not done for commercial gain or advantage of “a fine under this title or imprisonment for not more than six months, or both. . . .” 18 U.S.C. § 2701(b)(B).

**COUNT IV-. VIOLATION OF THE
CIVIL RIGHTS ACT (42 U.S.C. § 1983)**

48. Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

49. Section 1983 states in pertinent part:

Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity or other proper proceeding for redress. . . .

50. All Defendants are “persons” within the meaning of § 1983, in that at all times material hereto they were acting under the color of state law as a political subdivision of the Commonwealth of Pennsylvania, or a representative thereof.

51. Defendants’ clandestine remote activation of the webcams complained of deprived Plaintiff of his right to privacy as protected by the Fourth Amendment of the United States Constitution.

52. As Plaintiff first learned of Defendants’ unlawful deprivation of his privacy rights on June 8, 2010, this action has been commenced within §1983’s applicable two-year statute of limitations.

53. Defendants’ conduct in remotely activating the webcams complained of, which resulted in the deprivation of Plaintiff’s constitutionally protected right to privacy was intentional, extreme and outrageous, and thereby entitles Plaintiff to an award of punitive damages.

**COUNT V - INVASION OF
PRIVACY (U.S. CONST. AMEND. IV)**

54. Plaintiff repeats and re-alleges each and every preceding allegation as if fully set forth herein.

55. At a minimum, and pursuant to the Fourth Amendment of the United States Constitution, U.S. CONST. amend. IV, Plaintiff had a reasonable expectation of privacy with respect to the use of the webcams embedded in the laptop computers issued by the School District.

56. In particular, Plaintiff was never informed that the webcam incorporated into the students’ personal laptop computer could be remotely activated by the School District and/or its agents, servants, workers or employees indiscriminately at the whim of the School District, and

that such activation would naturally capture images of anything in front of the webcam at the time of its activation.

57. In as much as the personal laptop computers were used by students of the high schools and their families, it is believed and therefore averred that the School District has the ability to and has captured images of Plaintiff without his permission and authorization, all of which is embarrassing and humiliating.

58. As the laptops at issue were routinely used by students and family members while at home, it is believed and therefore averred that many of the images captured and intercepted may consist of images of minors and their parents or friends in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress.

**COUNT VI- PENNSYLVANIA WIRETAPPING AND
ELECTRONIC SURVEILLANCE ACT (18 PA. C.S.A. § 5101, *ET SEQ.*)**

59. Plaintiff repeats and re-alleges each and every preceding allegation as if fully set forth herein.

60. Section 5703 of the PWESA states in pertinent part:

Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:

1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or aural communication;

61. Section 5702 of the PWESA defines “intercept” to include the “aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. C.S.A. § 5702.

62. Section 5702 of the PWESA defines “electronic communications” to include “any transfer of signs, signals, writing, images, . . . transmitted in whole or in part by a wire, radio,

electromagnetic, photo electronic or photo optical system. . .“ 18 Pa. C. S.A. § 5702.

63. Section 5702 of the PWESA defines “person” as “any employee, or agents of the United States or any state or political subdivision thereof 18 Pa. C.S.A. § 5702.

64. Pursuant to § 5702 of the PWESA, Defendants are “persons” within the meaning of the Act, and Defendants’ conduct with respect to the webcams complained of constitutes an interception of electronic communications violative of the PWESA.

65. Pursuant to § 5725 of the PWESA:

Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

- 1) Actual damages, but not less than liquidated damages computed at the rate of \$100.00 a day for each day of violation, or \$1,000.00, whichever is higher.
- 2) Punitive damages.
- 3) A reasonable attorney’s fee and other litigation costs reasonably incurred.

**COUNT VII- INVASION OF
PRIVACY: PENNSYLVANIA COMMON LAW**

66. Plaintiff repeats and re-alleges each and every preceding allegation as if fully set forth herein.

67. At all times material hereto, and pursuant to the common law of Pennsylvania, Plaintiff had a reasonable expectation of privacy with respect to the operation of the webcams complained of.

68. Plaintiff was never informed of the School District’s capability and practice of remotely activating the webcams complained of.

69. As the laptops at issue were routinely used by the students, their friends and family members while at home, it is believed and therefore averred that many of the webcam images captured and/or intercepted consist of minors and/or their parents in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress.

WHEREFORE Plaintiff, JOSHUA LEVIN, requests judgment in theft favor and against Defendants, Lower Merion School District, The Board of Directors of the Lower Merion School District and Christopher W. McGinley, jointly and severally, as follows:

- 1) for compensatory damages;
- 2) for liquidated damages;
- 3) for punitive damages;
- 4) for attorneys' fees and costs;
- 5) for such other and further relief as this Court deems just and appropriate.

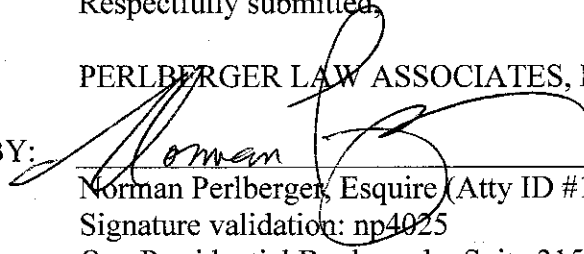
DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues for which a right to jury trial exists.

Respectfully submitted,

PERLBERGER LAW ASSOCIATES, P.C.

BY:


Norman Perlberger, Esquire (Atty ID #15742)

Signature validation: np4025

One Presidential Boulevard – Suite 315

Bala Cynwyd, PA 19004

(610)664-2440

perlberglaw@aol.com

Attorney for Plaintiff